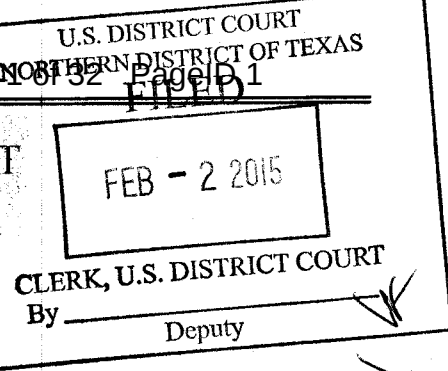


SEALED**UNITED STATES DISTRICT COURT**for the
Northern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

212 Rainsong Drive, Cedar Hill, Texas 75104-3150

Case No.

3-15-mj-053-BN

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
212 Rainsong Drive, Cedar Hill, Texas 75104-3150, as further described in Attachment A, which is attached and incorporated by reference.

located in the NORTHERN District of TEXAS, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHED AFFIDAVIT OF SPECIAL AGENT STEPHEN M. HANLEY

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 USC Section 1343

SEE ATTACHED AFFIDAVIT AND ATTACHMENTS

The application is based on these facts:

SEE ATTACHED AFFIDAVIT AND ATTACHMENTS

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Stephen M. Hanley, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 02/02/2015City and state: Dallas, Texas

Judge's signature

United States Magistrate Judge David L. Horan

Printed name and title

AFFIDAVIT OF STEPHEN M. HANLEY, SPECIAL AGENT

FEDERAL BUREAU OF INVESTIGATION

I, Stephen M. Hanley, a Special Agent with the Federal Bureau of Investigation ("FBI"), Dallas, Texas, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am an investigator and law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7). I am an officer of the United States, who is empowered to conduct investigations of, and make arrests for, the offenses enumerated in 18 U.S.C. §§ 1341 (mail fraud), 1343 (wire fraud), and 1956 (money laundering).

2. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") since 2002 and a federal law enforcement Agent since 1998. I am assigned to a squad in Dallas, Texas that is responsible for investigating complex financial crimes. While with the FBI, I have participated in the investigation of individuals and organizations involved in various white-collar and violent crimes, to include violations of various forms of fraud (government, insurance, health care, mail, wire, bank, investment, and corporate fraud), as well as tax evasion, money laundering, public corruption, civil rights (color of law, hate crimes and human trafficking), bank robbery, sexual assault, kidnapping and murder. These

investigations have often involved the use of physical surveillance, cooperating witnesses, financial and telephone toll record analysis, the execution of search and arrest warrants, and the debriefing of witnesses and subjects. I also have experience in the review of evidence obtained during the execution of a search warrant. I have received training in financial analysis, financial investigative methods, and applications, techniques for disguising and transmitting the proceeds of illegal activities, and asset forfeiture. I also have training regarding computers and digital evidence.

3. During my law enforcement career, I have written and/or executed numerous search, seizure, and arrest warrants pertaining to the seizure of various types of criminal evidence related to the commission of economic crimes. I have interviewed suspects and confidential informants regarding their facilitation of fraudulent schemes and white collar offenses.

4. Based on my training, experience, knowledge and participation in criminal investigations, and accumulated knowledge from consultations with other law enforcement agents, including debriefings and interviews of known offenders in other cases, I also know and contend that the following traits are common practices of offenders involved in various types of fraud:

- a. fraud is frequently a continuing activity over many months and even years;

- b. offenders who commit fraud keep records of their illegal activities for a lengthy period of time, even extending substantially beyond the time during which they actually produce, market, sell, and profit from their crimes;
- c. offenders who commit fraud commonly maintain hard copy and computer files, books, records, receipts, notes, ledgers, journals, diaries, address books, and other sundry materials, and papers relating to their crimes; and
- d. offenders who commit fraud often possess evidence, fruits, and instrumentalities relating to such offenses in their places of business, including home offices.

5. This affidavit is made in support of an application for a warrant to search the property located at 212 Rainsong Drive, Cedar Hill, Texas 75104-3150 (the "Premises"), as described more in Attachment A. I request authority to search the entire Premises, including the residential dwelling, any vehicles or curtilages/outbuildings or persons located on said property, and any computer (as defined in 18 U.S.C. § 1030(e)(1)) or other digital media storage device located therein, where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of the aforementioned wire-fraud crime.

6. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause that evidence, fruits, and instrumentalities of

violations of 18 U.S.C. § 1343 (wire fraud) are presently located on the Premises. This affidavit is based on my own personal knowledge, as well as information provided by records, databases and other law enforcement officers. Where statements of others are set forth in this affidavit, they are set forth in substance and in part. Special Agent Tim Schmitz ("SA Schmitz") in the FBI's Oklahoma City division has conducted many of the interviews in this investigation.

7. The FBI investigation has focused on Sandra Saldana ("Saldana"), also known as Vianna Gorman and Dominique Garza, doing business as GNS Electric, Inc. and Coverall Management, Inc. The investigation has indicated that there is probable cause to believe evidence, fruits, and instrumentalities of violations of 18 U.S.C. §1343 are located at the Premises.

THE INVESTIGATION

Paycom

8. Paycom is a payroll service company located in Oklahoma City, Oklahoma. For a fee, Paycom performs the payroll function for other entities.

9. On September 4, 2014, and September 12, 2014, SA Schmitz met with representatives of Paycom. During the meetings, Paycom employees reported that in July 2014, Paycom received an online request for a price quote from a person identifying herself as Vianna Gorman ("Gorman"). Paycom sent Gorman a price quote to the address gnselectric.vianna@gmail.com, which Gorman had

provided as the contact email address. Using the gnselectric.vianna@gmail.com address, Gorman requested Paycom to begin the client setup process. Gorman advised Paycom that she was the office manager of GNS Electric, Inc. ("GNS"), 3200 Lancaster Road, Dallas, Texas 75217, that her office telephone number was (214) 614-8204, and her fax number was (469) 533-6486. Gorman emailed Paycom, using the gnselectric.vianna@gmail.com address, three items: (1) a copy of a letter from the Internal Revenue Service ("IRS"), indicating GNS's Taxpayer Identification Number was xx-xxx6643, (2) a copy of a voided GNS check drawn on account number xxxxxx3713 at Bank of Texas, and (3) an Excel spreadsheet with the name, social security number, date of birth, address, pay type, pay rate, marital status, exemptions, type of account, routing number, and bank account number for each purported GNS employee.

10. From August 5, 2014, to August 20, 2014, Gorman initiated contact with Paycom's application software on at least 21 occasions, using Internet Protocol ("IP") address 107.138.133.212. From August 26, 2014, to September 3, 2014, Gorman initiated contact with Paycom's application software on at least eight occasions, using IP address 107.138.135.33. During August 2014, Paycom initiated ACH debits, totaling approximately \$223,000, from Bank of Texas account number xxxxxx3713 to fund what Gorman represented to be GNS's

payroll. Paycom subsequently learned the bank accounts funded were actually prepaid debit card accounts.

11. On September 2, 2014, Paycom received a telephone call from GNS employee Brenda Stanfer ("Stanfer"). Stanfer called Paycom to ask why Paycom made tax deposits on GNS's behalf. Paycom advised Stanfer that Gorman initiated contact with Paycom to conduct GNS's payroll function. Stanfer advised Paycom that GNS did not have an employee by the name of Vianna Gorman, and it did not initiate contact with Paycom.

12. On September 25, 2014, SA Schmitz interviewed Evelyn Gorman ("Evelyn"), the owner of GNS. Evelyn advised that in March 2013, GNS moved from 3200 Lancaster Road, Dallas, Texas, to 430 West Jefferson Boulevard, Suite 102, Dallas, Texas 75208.

Around December 3, 2013, Evelyn hired Saldana, DOB xx-xx-1976, social security number xxx-xx-1426, as a Senior Accountant. At the time of her GNS employment, Saldana advised Evelyn that she resided with her girlfriend, Mary Ann Cervantes ("Cervantes"), at 2740 South Polk Street, Dallas, Texas 75224. Saldana further advised Evelyn that her cellular telephone number was (214) 516-3586. Saldana's position at GNS allowed her access to all of GNS' accounting and banking records.

In February 2014, Evelyn discovered several unauthorized charges on GNS's Amazon account. The unauthorized charges ranged from \$30.00 to \$50.00 and totaled \$635.00. Evelyn questioned Saldana about the unauthorized Amazon charges, and Saldana admitted the email address used to make the Amazon purchases belonged to her. Saldana then advised she had a family emergency and left GNS and never returned.

After learning of the unauthorized Amazon charges, Evelyn discovered several GNS checks payable to Saldana, with a forged signature for Evelyn. The checks totaled approximately \$12,000. Evelyn filed a report with the Dallas Police Department regarding the forged checks.

Representatives from two other payroll companies—PaySphere and PayDayPro, LLC ("PayDayPro")—contacted Evelyn in 2014. Both companies advised Evelyn that a person identifying herself as Vianna Gorman initiated contact with their respective companies to conduct GNS's payroll. Evelyn advised both companies that GNS had not initiated contact with their company and that GNS did not have an employee by the name of Vianna Gorman. The PayDayPro representative provided Evelyn with a copy of the same voided check and Excel spreadsheet that Gorman had provided to Paycom.¹

¹ SA Schmitz has interviewed representatives of PaySphere and PayDayPro, and confirmed that a person identifying herself as Vianna Gorman contacted those companies in July 2014 to set up payroll for GNS. SA Schmitz has also

Evelyn later contacted Bank of Texas and learned the voided check sent to Paycom and PayDayPro was drawn on an account belonging to Pogue Construction. GNS subsequently contacted Pogue Construction.

GNS employees do not use Gmail email accounts to conduct GNS business. Evelyn's email account is evelyn@gnselectricinc.com. GNS employees use email accounts with the domain gnselectricinc.com.

13. On September 26, 2014, SA Schmitz interviewed Deborah Horton, Accounting and Office Manager, Pogue Construction ("Pogue"). Horton advised that in late August or early September 2014, GNS contacted Pogue and advised it had discovered its tax deposits were overpaid and that Pogue had made deposits on GNS's behalf. Pogue checked its bank account and discovered Paycom had initiated approximately \$200,000 of withdraws from its Bank of Texas account number xxxxxx3713. Pogue did not authorize Paycom to initiate withdraws from this account.

interviewed a representative from Evans Payroll, who reported a similar contact by Gorman in July 2014. Gorman requested a price quote from all three companies using the e-mail address of gnselectric.vianna@gmail.com. Gorman provided Evans Payroll and PayDayPro the same voided check that Gorman provided to Paycom. The three companies did not process any payroll, after learning that GNS did not have an employee named Gorman and that GNS had not initiated contact with their company.

14. SA Schmitz has reviewed the file properties associated with the Excel spreadsheet that Gorman provided to Paycom. The properties indicate the author of the Excel file to be Saldana.

15. Pursuant to a Federal Grand Jury subpoena, Bank of Texas provided records for Pogue Construction's Bank of Texas account number xxxxxx3713. The records indicate Paycom initiated ten withdrawals, totaling \$223,095.31 from August 7, 2014, to August 28, 2014.

16. On January 26, 2014, SA Schmitz spoke with Tom Bubb and Lauren Toppins of Paycom. They advised that from on or about August 6, 2014 to August 28, 2014, Paycom, through its bank account at PNC Bank in Pittsburgh, Pennsylvania, conducted ten ACH withdraws, totaling approximately \$223,000, from Pogue's Bank of Texas account number xxxxxx3713, in Dallas. During the same period, Paycom sent approximately eight electronic communications from its Oklahoma City headquarters to PNC Bank in Pittsburgh, instructing PNC to conduct the ACH withdraws from Pogue's Bank of Texas account.

IP Addresses and Phone Records Connected to Saldana

17. Pursuant to a Federal Grand Jury subpoena, on November 24, 2014, AT&T provided subscriber information for IP addresses 107.138.133.212 and 107.138.135.33. Both IP addresses were assigned to a person identified as Betty Graciano ("Graciano") with telephone number (214) 516-3586, the same telephone

Saldana provided Evelyn, as identified in paragraph 12. Graciano's e-mail address was mandmtaxservices2012@gmail.com. AT&T service was established on April 30, 2013.

From at least March 17, 2014 to August 24, 2014, AT&T assigned Graciano with IP address 107.138.133.212. From August 25, 2014 to at least November 24, 2014, AT&T assigned Graciano with IP address 107.138.135.33.

The physical service location for Graciano's AT&T Internet service from at least November 9, 2013, to April 21, 2014, was 2814 Sunset Strip Drive, Glenn Heights, Texas 75154. From April 22, 2014, to September 11, 2014, the service location was 3708 Oak Creek Circle, Dallas, Texas 7522. From September 12, 2014, to at least November 24, 2014, the service location was 212 Rainsong Drive, Cedar Hill, Texas 75104.

18. Pursuant to a Federal Grand Jury subpoena, J2 Global, Inc. ("J2") provided records for telephone number (214) 614-8204, identified in paragraph 9. The records indicate the subscriber to be GNS Electric, 2814 Sunset Strip Avenue, Glenn Heights, Texas 75154. The business telephone number associated with the account is (817) 224-2941. The email address associated with the account is gnselectric.vianna@gmail.com. From July 22, 2014, to August 6, 2014, approximately 40 calls to telephone number (214) 614-8204 were transferred to number (214) 516-3586, the same telephone number Saldana provided to Evelyn.

19. Pursuant to a Federal Grand Jury subpoena, J2 also provided records for telephone number (469) 533-6486, identified in paragraph 9. The records indicate the subscriber to be Sandra Saldana, 3708 Oak Creek Circle, Dallas, Texas 75227. The telephone number associated with the account was (817) 224-2941. On July 9, 2014, IP address 107.138.133.212 was used to register the account with J2. On July 9, 2014, IP address 107.138.133.212 was assigned to Graciano with telephone number (214) 516-3586, the same number Saldana provided to Evelyn.

The Premises and Saldana's Former Residences

20. Pursuant to Federal Grand Jury subpoena, American Homes 4 Rent provided records associated with 212 Rainsong Drive, Cedar Hill, Texas 75104, the most recent service address for IP address 107.138.135.33. The records indicate American Homes 4 Rent leased Saldana the property on September 11, 2014. The term of the lease is September 11, 2014 to August 31, 2015. Saldana's application indicates her telephone number to be (214) 516-3586, the same telephone number identified in paragraph 12, and her previous address to be 3708 Oak Creek Circle, Dallas, Texas 75227. On the rental application, Saldana identified her vehicle as a 2013 black Merceden (sic) Benz, ML 350.

The rental records further indicate Saldana's son and daughter—M.S., DOB xx-xx-1998, and M.S., DOB xx-xx-1999—also reside at the property. Saldana's reference and emergency contact is Mary Ann Cervantes, 2814 Sunset Strip

Avenue, telephone number (469) 278-1950. Saldana did not provide a city, state and zip code for Cervantes. The residences located at 2814 Sunset Strip and 3708 Oak Creek Circle are the same addresses identified by AT&T as the service locations for IP addresses 107.138.133.212 and 107.138.135.33, identified in paragraph 17.

21. On January 14, 2015, SA Schmitz interviewed Steven Stanford ("Steven"). He stated that his father, David Stanford, owns 2814 Sunset Strip Avenue, Glenn Heights, Texas 75154. Steven manages the property. Sandra Saldana leased the property from November 1, 2013 to May 2014. Saldana's son—M.S.—and daughter—M.S.—also lived in the property. Betty Graciano has never been a tenant of the property or any property managed by Steven.

22. On January 14, 2015, SA Schmitz interviewed Roger Maker ("Maker"). Maker relayed that he owns 3708 Oak Creek Circle, Dallas, Texas 75227. Sandra Saldana leased the property from March 14, 2014, to September 2014. Saldana's son and daughter—M.S. and M.S.—lived at the property with Saldana. Saldana provided Marker with Mary Ann Cervantes, telephone number (469) 278- 1950, as Saldana's emergency contact. Maker does not know Graciano. Maker never leased the property to Graciano.

23. On January 29, 2015, SA Schmitz confirmed with American Homes 4 Rent that Saldana is still the registered tenant of 212 Rainsong Drive, Cedar Hill,

Texas 75104. Also, on January 21, 2015, I drove by the Premises and saw Saldana's vehicle parked in the driveway of the Premises.

Fraudulent Wire Transfers and Transactions of Purported GNS Employees

24. SA Schmitz has reviewed Paycom banking records associated with Paycom's processing of payroll for purported GNS employees. Two of the purported GNS employees receiving funds were Adalberto Gonzalez ("Gonzalez") and Brandon Hatchel ("Hatchel").

On or about August 7, 2014, Paycom direct deposited \$1,557.43, and \$1,567.11, in Gonzalez's Metabank account number xxxxxxxxxx5178. On or about August 21, 2014, and August 26, 2014, Paycom direct deposited \$1,721.81 and \$1,876.51, respectively, to the same account. On or about August 7, 2014, and August 21, 2014, Paycom direct deposited \$1,341.27 and \$1,699.02, in Hatchel's Metabank account number xxxxxxxxxx2920.

25. On January 14, 2015, SA Schmitz again interviewed Evelyn, the owner of GNS. Evelyn stated that GNS has never had an employee by the name of Adalberto Gonzalez, and GNS had a former employee by the name of Brandon Hatchel. Hatchel's address at the time of his GNS employment was in Kaufman, Texas, and he reported a telephone number of (469) xxx-3401.

26. Pursuant to a Federal Grand Jury subpoena, Metabank provided bank records for the above-described accounts in the name of Gonzalez and Hatchel.

Gonzalez's account was created on December 24, 2013. According to account records, Gonzalez's mailing address was 2814 Sunset Strip Avenue, Red Oak, Texas 75154, the same street address and zip code associated with the service location of IP address 107.138.133.212, identified in paragraph 17. Gonzalez's telephone number was (214) 516-3586, the same telephone Saldana provided Evelyn and American Homes 4 Rent. On June 2, 2014, June 28, 2014, and August 9, 2014, Cirro Energy debited \$145.87, \$201.53 and \$220.25 respectively, from Gonzalez's account. On August 30, 2014, Southwest Airlines debited \$2,437.20 from Gonzalez's account.²

MetaBank records indicate that on September 2, 2014, at approximately 9:21 AM, Central Standard Time, a \$303.00 withdraw was made from Gonzalez's account at the J.P. Morgan Chase ("Chase") Automated Teller Machine located at 1345 North Town East Boulevard, Mesquite, Texas.

MetaBank records further indicate that Hatchel's account was created on January 19, 2014. Hatchel's mailing address is 2814 Sunset Strip Avenue, Red Oak, Texas 75154, the same street address and zip code for the service location of IP address 107.138.133.212, identified in paragraph 17. Hatchel's telephone

² In addition to the Paycom deposits for GNS Electric, Gonzalez's Metabank account contained deposits from the Internal Revenue Service, Ted's Auto Corporation, Coverall Management and Payroll Data Pro. The \$5,792.00 deposit from Internal Revenue Service on May 11, 2014 may indicate a false tax return and rebate under Gonzalez's name.

number was (469) 852-3098. Hatchel's email address was tedsautocorp@gmail.com.

On June 30, 2014, the City of Dallas debited \$92.24 from the Hatchel account.³ In addition, on September 4, 2014, Hatchel's account had a withdrawal of \$685.32 from M & M Tax Services. The transaction on the bank statement associates M & M Tax Services with telephone number (214) 516-3586, the same number identified with Graciono's AT&T service and the same number that Saldana provided to Evelyn and American Homes 4 Rent.⁴

27. On January 20, 2015, Chase provided SA Schmitz with photos of the individual conducting the \$303.00 withdraw from Gonzalez's account, as referenced in paragraph 26. The Chase photos depict a female, driving a black Mercedes Benz Sport Utility Vehicle. SA Schmitz compared the Chase photos to Saldana's Texas driver's license photo, which I provided to him during the investigation, as well as photos of Saldana obtained from a Facebook profile under her name. SA Schmitz believes the Chase photos to be Saldana after comparing those photos to Saldana's Texas driver's license photo and the Facebook photos. SA Schmitz has also compared a picture of a 2013 Mercedes Benz ML 350, the

³ In addition to Paycom's deposits for GNS Electric, Hatchel's Metabank account contained deposits from Coverall Management and Payroll Data Pro.

⁴ Several bank accounts associated with this payroll scheme include withdraw entries involving M & M Tax Services and the (214) 516-3586 telephone number. Withdraws to M & M Tax Service may indicate a scheme to launder money from the fraudulent accounts.

vehicle Saldana provided in her American Homes 4 Rent application to the black Mercedes Benz SUV, depicted in the Chase photos, and he believes the vehicle in the Chase photos to be a Mercedes Benz ML 350.

28. Cirro Energy advised FBI that the three debits to Gonzalez's account, identified in paragraph 26, were payments to Cirro Energy account number xxxx8348, registered to Sandra Saldana, 3708 Oak Creek Circle, Dallas, Texas 75227, the same address Saldana reported American Homes 4 Rent to be her previous address. The home telephone number associated with the account is (214) 516-3586, the same telephone number Saldana provided to Evelyn and American Homes 4 Rent.

29. Pursuant to a Federal Grand Jury subpoena, Southwest Airlines provided records for the \$2,437.20 charge to Gonzalez's account. The records showed that on August 29, 2014, Sandra Saldana, Mary Anne Cervantes, Saldana's son and daughter, and two other persons traveled on Southwest Airlines from Dallas to San Antonio. On September 1, 2014, they returned to Dallas. The billing name associated with the travel was Sandra Saldana. A travel itinerary was emailed by Southwest Airlines to sandrasaldana1976@gmail.com.

30. On January 14, 2015, SA Schmitz interviewed Brandon Hatchel ("Hatchel"). Hatchel stated that he was employed with GNS in 2008 or 2009. Hatchel was fired from GNS for not meeting Evelyn's expectations. Hatchel has

never had a prepaid MasterCard from Metabank. Hatchel has never used the mailing address 2814 Sunset Strip Avenue, Red Oak, Texas 75154, the telephone number (469) 852-3098, or the email address tedsautocorp@gmail.com.

31. The City of Dallas provided records for its \$92.24 charge to Hatchel's bank account, identified in paragraph 26. The records indicate the charge was payment to water account number xxxxx2893, registered to Mary Ann Cervantes, 3708 Oak Creek Circle, Dallas, Texas 75227.

Coverall Management

32. The investigation has further indicated that Saldana has attempted to defraud payroll companies by representing herself as Dominique Garza with Coverall Management.

33. On November 18, 2014, SA Schmitz interviewed David Volpi, of Payroll Data Processing ("PDP"), Tampa, Florida. Volpi stated that in July 2014, Dominique Garza, using email address dominique.coverallmanagement@gmail.com, contacted PDP to setup payroll for Coverall. Garza advised she was the Coverall owner's daughter as well as Coverall's bookkeeper/controller. Garza provided PDP with a letter from the IRS, identifying Coverall's EIN. Garza also provided Capital One bank account number xxxxxx6999 as the account from which PDP was to withdraw funds to process Coverall's payroll. PDP processed four payrolls for Coverall, totaling

approximately \$132,000. After the fourth payroll, PDP received a call from its bank advising funds to cover the fourth payroll were not available. PDP contacted Coverall employee Christie Proctor ("Proctor"), and Proctor advised PDP that Coverall had not contracted with any payroll company for its payroll. Proctor further advised PDP that Coverall had terminated an employee by the name of Sandra Saldana in September or October 2013 for embezzlement. During Saldana's employment with Coverall, she had access to all of Coverall's corporate information.

34. On November 19, 2014, SA Schmitz interviewed Christie Proctor. Proctor advised that Saldana was employed with Coverall as a bookkeeper from January 2013 to May 31, 2013. While employed with Coverall, Saldana had access to all of Coverall's corporate information, including its EIN. During Saldana's employment with Coverall, she was married to Mary Ann Cervantes.

Saldana resigned from Coverall after her hours were reduced. Following Saldana's departure, Coverall was contacted by several payroll companies, inquiring as to whether Coverall had initiated contact with them to conduct Coverall's payroll. Proctor advised the payroll companies that Coverall had not contracted with anyone to conduct its payroll function.

35. On November 24, 2014, SA Schmitz interviewed Ken Cash, Senior Fraud Investigator, Capital One, N.A. He advised account number xxxxxx6999

belonged to Nova Asset Management (“NAM”), and that NAM was the victim of approximately \$138,000 in unauthorized debits from its account by two payroll companies.

36. On November 18, 2014, SA Schmitz interviewed Anthony Maniscalco (“Maniscalco”) of 1-2-3 Payroll (“1-2-3”) in Holtsville, New York. Maniscalco relayed that in November 2014, Garza, using the email address dominique.coverallmanagement@gmail.com, contacted 1-2-3. Garza advised she was the Office Manager for Coverall, 1200 South Main Street, Ft. Worth, Texas 76110 with telephone number (817) 224-2941, the same telephone number identified in paragraphs 17 and 18. Garza provided 1-2-3 with (1) a copy of a letter from the IRS, indicating Coverall’s Taxpayer Identification Number was xx-xxx1700, the same letter provided to PDP, (2) an Excel spreadsheet identifying Coverall’s purported employees, and (3) a copy of a check drawn on account number xxxxxx1522 at Comerica Bank. SA Schmitz reviewed the properties associated with the Excel file and discovered Saldana was the author. 1-2-3 processed one payroll for Coverall. Soon after that, Maniscalco spoke with Coverall and stopped further payroll activities. 1-2-3 did not sustain any loss.

37. On November 19, 2014, SA Schmitz interviewed Luciano Ramirez, Jr., of Macias Payroll Services (“MPS”) in San Antonio. Ramirez stated that around July 2014, Garza contacted MPS, using the address

dominique.coverallmanagement@gmail.com, to conduct Coverall's payroll. Garza provided MPS with (1) a copy of a letter from the IRS, indicating Coverall's Taxpayer Identification Number was xx-xxx1700, the same letter provided to PDP and 1-2-3, (2) a copy of a cancelled Coverall check drawn on account number xxxxxx6999 at Capital One, N.A., and (3) an Excel spreadsheet identifying Coverall's purported employees. SA Schmitz reviewed the properties associated with the Excel file and discovered Saldana was the author. Before processing payroll for Coverall, Ramirez spoke with Coverall and learned that Garza was not a Coverall employee. MPS did not process payroll for Coverall.⁵

38. SA Schmitz has also interviewed representatives of additional payroll companies that Garza contacted to perform Coverall's payroll. In July 2014, Garza contacted AmCheck, a payroll company in Austin, Texas, by using the e-mail address of dominique.coverallmanagement@gmail.com. In July 2014, AmCheck processed one payroll for Coverall. The payroll was processed by direct deposit to

⁵ During the interview on November 19, 2014, Ramirez further stated to SA Schmitz that around October 2014, individuals purporting to be Tonya Strong and Kelly Bates ("Bates") contacted MPS to conduct payroll for Manufactured Metals. They used the e-mail address of tonyas.manufacturedmetals@gmail.com. Bates provided MPS with (1) a copy of a letter from the IRS with Manufactured Metal's Taxpayer Identification Number, (2) a copy of a voided Manufactured Metals check, and (3) an Excel spreadsheet identifying Manufactured Metals' purported employees. SA Schmitz has reviewed the properties associated with the Excel file and discovered Saldana was the author. Ramirez contacted Manufactured Metals, learned it had not contracted with any payroll company to perform its payroll function, and did not complete the payroll request.

prepaid debit cards, supposedly belonging to Coverall employees. After processing the payroll, AmCheck learned funds were not available in the account Garza had provided to cover Coverall's payroll. AmCheck attempted to reverse the direct deposits but the funds were gone. AmCheck lost approximately \$14,000.

39. Garza also contacted Nevada Payroll Services ("NPS") and Paycor. In separate interviews with SA Schmitz, NPS and Paycor representatives advised that they contacted Coverall before processing any payroll, and learned that Coverall had not contracted with any payroll company to conduct its payroll. NPS and Paycor did not process any payroll for Coverall. In August 2014, Garza provided to Paycor account information for Pogue Construction as the account to withdraw funds to pay Coverall's payroll. This is the same account information that Gorman provided to Paycom to process GNS's payroll.

Recent Fraudulent Payroll Transfers

40. The investigation has indicated Saldana's involvement with a fraudulent payroll scheme has continued well after she moved to the Premises.

41. On January 9, 2015, SA Schmitz interviewed Matt Miley ("Miley") of Payout USA in Tallahassee, Florida. Miley relayed that in November 2014, Payout USA was contacted by Maria Rosales, using email address maria.pogueconstruction@gmail.com, to setup payroll for Pogue Construction. Rosales advised Payout USA that she was Pogue's officer manager. Rosales

provided bank account number xxxxxx3713 as the account from which Payout USA was to withdraw funds to cover Pogue's payroll. This was the same account that Gorman had provided to Paycom and that Garza had provided to Paycor.

In December 2014, Payout USA processed Pogue's first payroll, using direct deposit. Payout USA attempted to direct deposit approximately \$72,000 to bank accounts for reported Pogue employees. Approximately \$22,000 was returned to Payout USA for invalid bank account numbers. After funding the supposed Pogue employees, Payout USA was advised by their ACH provider that Payout USA was not authorized to withdraw funds from account number xxxxxx3713. Miley contacted Rosales, and Rosales advised she inadvertently provided the wrong account number. Rosales then provided two additional account numbers. Miley contacted the banks associated with the two additional accounts and learned both accounts were invalid. Payout USA has sustained a loss of approximately \$50,000 as a result of processing Pogue's payroll.

42. On December 9, 2014, SA Schmitz interviewed Doug Tanner ("Tanner") of Corporate Payroll Services ("CPS") in Norcross, Georgia. Tanner stated that in December 2014, CPS processed one payroll for Coverall. The payroll was conducted by check. CPS cut checks payable to purported Coverall employees. The checks were drawn on Comerica Bank account number xxxxxx1522. CPS mailed the checks, totaling approximately \$50,000, to Coverall

Management Association, Dominique Garza, 1200 South Main Street, Fort Worth, Texas 76110. The checks were returned as undeliverable. CPS conducted two ACH debits from account number xxxxxx1522, totaling approximately \$13,500 to cover payroll taxes and CPS's processing fee. CPS reversed the two ACH debits totaling \$13,500, upon notice of fraud. CPS did not sustain any loss.

Nature of Fraudulent Transactions with Unauthorized Payroll Funds

43. SA Schmitz has reviewed bank records for approximately 30 prepaid debit cards associated with Saldana's fraud. The records indicate Saldana received direct deposits to the prepaid debit cards, totaling approximately \$213,000. Approximately \$121,000 was withdrawn in cash, at various Automated Teller Machines. Approximately \$45,000 relates to Point of Sale transactions, which include the above-described debits to Cirro Energy, Southwest Airlines, the City of Dallas, and M & M Tax Services, as identified in paragraph 26.

Computer Evidence

44. I know that computer hardware, software, and electronic files may be important to a criminal investigation in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain evidence, instrumentalities, or fruits of crime in the form of electronic data. Fed. R. Crim. P. 41 permits the government to search for and seize computer hardware, software, and electronic

files that are evidence of crime, instrumentalities of crimes, and/or fruits of crime.

In this case, with respect to the Premises, the warrant application requests permission to search and seize evidence of wire fraud, including evidence that almost certainly was created on, and may now be stored on, a computer. I believe that the computer hardware sought is a container of evidence, and also itself an instrumentality of the crime under investigation.

45. Based on my knowledge, training, and experience, including the experience of other agents with whom I have spoken, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

46. Based upon my training, experience, and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, compact disks, and memory chips. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

- a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.
- b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain

procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

- c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 160 gigabytes (GB) of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 80 million pages of data, which, if printed out, would result in a stack of paper over four miles high.
- d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, or instrumentalities of a crime.

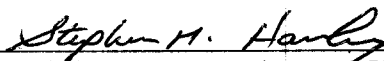
47. In light of these concerns, I request permission to seize any computer hardware (and associated peripherals) from the Premises that are believed to

contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the computer hardware on-site for the evidence.

CONCLUSION

48. Based on the above information, I respectfully submit there is probable cause to believe the Premises, located at 212 Rainsong Drive, Cedar Hill, Texas 75104-3150, maintains evidence of a violation of 18 U.S.C. §1343, in connection with a scheme to solicit payroll funds by false representations using interstate wires. The items listed in Attachment B are evidence of these crimes, contraband, fruits of these crimes, or property which is or has been used as the means of committing the foregoing offense.

Therefore, I respectfully request that a search warrant be issued, authorizing the search of the Premises described in Attachment A, and for the seizure of the items listed in Attachment B.


Special Agent Stephen M. Hanley
Federal Bureau of Investigation

Subscribed to and sworn before me this 26 day of February, 2015.


David L. Horan
United States Magistrate Judge

ATTACHMENT A:

PREMISES TO BE SEARCHED

The property located at 212 Rainsong Drive, Cedar Hill, Texas 75104-3150, including the main residence, and any vehicles or curtilage/outbuildings or persons located on said property.

The Premises includes a two-story, red brick home with cream-colored trim, a cream-colored front door, two cream-colored garage doors, and a black asphalt shingle roof. The numbers "212" are displayed with black numbers in a light-colored stone, centered above the garage on the front of the home.



The Premises is on the south side of the street, between 208 Rainsong Drive and 216 Rainsong Drive. The home faces north and is the third house on the right of Rainsong Drive if approaching from the west, and the fourth house on the left of

Rainsong Drive if approaching from the east. There are several windows on the front of the property, including a large, arched window above the front door and a narrow window on each side of the front door.

ATTACHMENT B:

SPECIFIC ITEMS TO BE SEIZED FROM THE PREMISES

1. Any computer (as defined in 18 U.S.C. § 1030(e)(1)), computer hardware, or other digital media storage device, consisting of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data, that agents determine are likely to contain files within the scope of the warrant. Hardware includes, but is not limited to, any data-processing devices (such as central processing units, self-contained "laptop" or "notebook" computers, "palm pilots", I-pods, cellular telephones, memory facsimile machines and "schedulers"); internal and peripheral storage devices (such as fixed disks, external hard drives, floppy disk drives and diskettes, USB storage devices, optical storage devices, read/write CD and DVD devices, and any storage devices); peripheral input/output devices (such as keyboards, printers, scanners, video display monitors, mouse devices); and related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

2. Computer software, that is, digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like word processing, networking, graphics, accounting, presentations or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

3. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and any passwords, password files, test keys, encryption codes or other information necessary to access the digital device or data stored on the digital device.

4. Any and all documents, whether in hard copy or electronic format, related to a payroll service or payroll company, including but not limited to Paycom, PaySphere, PayDay Pro, Evans Payroll, Payroll Data Processing, 1-2-3 Payroll, Macias Payroll Services, AmCheck, Nevada Payroll Services, Paycor, and Corporate Payroll Services.

5. Any and all documents, whether in hard copy or electronic format, related to GNS Electric, Pogue Construction, Coverall Management, Manufactured Metals, and M & M Tax Services.

6. Any United States currency.

7. Any and all records, whether in hard copy or electronic format, for merchandise purchases after January 1, 2013.

8. Any and all ATM receipts after January 1, 2013.

9. Any and all bank records for any checking, savings, or loan accounts after January 1, 2013.

10. Any and all debit, credit or ATM cards.

11. Any and all false identification documents, counterfeit access devices, and unauthorized access devices including, but not limited to, counterfeit passports, drivers licenses, Social Security cards, credit cards, birth certificates, checks, and tax returns; and stolen or fraudulent credit card numbers, debit card numbers, bank account numbers, and automated teller machine card personal identification numbers.

12. Any and all forms of identification, issued by whatever government or private entity, including any names and/or visual likenesses found therein.

13. Any and all equipment and supplies that can be used to manufacture, counterfeit, alter, or modify credit or debit cards.